



UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/646,489	11/02/2000	Edward J. Naclerio	770P009665-U	8816
2512	7590	02/09/2005	EXAMINER	
PERMAN & GREEN 425 POST ROAD FAIRFIELD, CT 06824			WOO, RICHARD SUKYOON	
			ART UNIT	PAPER NUMBER
			3629	

DATE MAILED: 02/09/2005

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary

Application No.

09/646,489

Applicant(s)

NACLERIO

Examiner

Richard Woo

Art Unit

3629

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --
Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

- 1) ☒ Responsive to communication(s) filed on 19 November 2004.
- 2a) ☐ This action is FINAL. 2b) ☒ This action is non-final.
- 3) ☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

- 4) ☒ Claim(s) 2 and 4-21 is/are pending in the application.
- 4a) Of the above claim(s) _____ is/are withdrawn from consideration.
- 5) ☐ Claim(s) _____ is/are allowed.
- 6) ☒ Claim(s) 2, 4-18 and 21 is/are rejected.
- 7) ☒ Claim(s) 19 and 20 is/are objected to.
- 8) ☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

- 9) ☐ The specification is objected to by the Examiner.
- 10) ☐ The drawing(s) filed on _____ is/are: a) ☐ accepted or b) ☐ objected to by the Examiner.
Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).
Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).
- 11) ☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

- 12) ☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
- a) ☐ All b) ☐ Some * c) ☐ None of:
1. ☐ Certified copies of the priority documents have been received.
2. ☐ Certified copies of the priority documents have been received in Application No. _____.
3. ☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

- 1) ☒ Notice of References Cited (PTO-892)
- 2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
- 3) ☐ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08)
Paper No(s)/Mail Date _____.
- 4) ☐ Interview Summary (PTO-413)
Paper No(s)/Mail Date: _____.
- 5) ☐ Notice of Informal Patent Application (PTO-152)
- 6) ☐ Other: _____.

DETAILED ACTION

Response to Arguments

- 1) The applicant's response, filed November 19, 2004, has been entered.
- 2) Applicant's arguments, filed November 19, 2004, with respect to the prior art rejection have been fully considered and are persuasive. The previous rejection of claims under 35 U.S.C. 103 has been withdrawn.
- 3) The text of those sections of Title 35, U.S. Code not included in this action can be found in a prior Office action.

Claim Objections

- 4) Claim 8 is objected to because of the following informalities:
In Claim 8, line 5, "a" before 'administrator' should be changed to --an--.
Appropriate correction is required.

Claim Rejections - 35 USC § 103

- 5) Claims 2, 4, 6, 9-10, and 12-16 are rejected under 35 U.S.C. 103(a) as being unpatentable over Rager et al. (US 5,363,447) in view of Grider et al. (US 5,515,540).

W.R.T. Claim 2:

Rager et al. discloses a method comprising the steps of:
storing the encryption key within the second memory (106, in Fig. 1; col. 4, lines 17-20);

Art Unit: 3629

encrypting the body of data by the cryptographic engine (105) with respect to the encryption key (col. 3, lines 27-34);

storing the encrypted body of data in the first memory (103 in Fig. 1, col. 4, lines 8-10);

upon power-up of the security device decrypting the encrypted body of data with the cryptographic engine with respect to the encryption key (col. 4, lines 23-27);

temporarily storing the decrypted body of data in a third memory (102 in Fig. 1; col. 4, lines 31-32, 35-36), wherein upon power down of the device the decrypted body of data is lost; and

in the event of tampering with the device, removing power from the second memory resulting in a loss of the encryption key and the decrypted body of data (see col. 4, lines 44-49).

However, Rager et al. does not expressly disclose the method further including:

in the event of tampering with the PSD, removing power from the third memory resulting in a loss of the decrypted body of data.

Grider et al. teaches for, a security improvement against tempering, that the improvement includes: a micro-controller supplies power to the memory either from a system power supply or from the battery, and grounds the power-output to the memory to destroy all data in the memory (col. 2, lines 1-6).

Since Grider et al. and Rager et al. are both from the same field of endeavor of providing security measure against tempering for the memory, the purpose disclosed by Grider et al. would have been well recognized in the pertinent field of Rager et al..

Accordingly, it would have been obvious at the time the invention was made to a person having ordinary skill in the art, to not only remove power from the second memory, which is supplied with the power even after the device is powered down, but also remove the power from the third memory, which is only supplied with the power during the power ups of the device, as taught by Grider et al., for the purpose of providing a device with improved security against tempering, including attempts at active intrusion while the machine is running (Rager et al. already prevents the device from tempering when powered downs and with teaching of Grider et al. the modified Rager et al. can further prevent the tempering against active intrusion during the power ups).

W.R.T. Claim 4:

Rager et al. discloses a device comprising:

a second volatile memory (106) for storing the encryption key (in Fig. 1; col. 4, lines 17-20), wherein a constant voltage is supplied to the encryption device and consequently to the second memory (col. 4, lines 37-40) when the device is powered down;

a first nonvolatile memory (130) not having a backup power batter for storing the encrypted body of data in the first memory (103 in Fig. 1, col. 4, lines 8-10);

Art Unit: 3629

an encryption engine (105) for encrypting the body of data with respect to the encryption key (col. 3, lines 27-34);

a third memory not having a backup battery for temporarily storing the decrypted body of data (102 in Fig. 1; col. 4, lines 31-32, 35-36); and

wherein upon power down of the device the decrypted body of data in the third memory is lost.

However, Rager et al. does not expressly disclose what kind of backup power is supplied to the second memory device (is it a backup battery power source or other power source?).

Grider et al. teaches for, a security improvement against tempering, that the improvement includes: the memory is getting power source either from a system power supply or from the backup battery (col. 2, lines 1-6).

Since Grider et al. and Rager et al. are both from the same field of endeavor of providing security measure against tempering for the memory, the purpose disclosed by Grider et al. would have been well recognized in the pertinent field of Rager et al..

Accordingly, it would have been obvious at the time the invention was made to a person having ordinary skill in the art, to supply power to second memory from the backup battery in case the device is powered down, as taught by Grider et al., for the purpose of maintaining security while the security device is powered down.

The modified device of Rager et al. discloses the invention as recited above, but does not specifically disclose that the second memory is a nonvolatile type.

At the time the invention was made, it would have been an obvious matter of design choice to a person of ordinary skill in the art to substitute the nonvolatile memory in place of the volatile memory because Applicant has not disclosed that utilizing the nonvolatile memory instead of volatile one provides an advantage, is used for a particular purpose, or solves a stated problem. One of ordinary skill in the art, furthermore, would have expected Applicant's invention to perform equally well with the second volatile memory of Rager et al. because the data in the second volatile memory of Rager et al. will also be erased if the device is tempered.

Therefore, it would have been an obvious matter of design choice to further modify the modified device of Rager et al. to obtain the invention as specified in claim.

W.R.T. Claim 6: The modified device of Rager et al. discloses the invention as recited above, but does not expressly disclose the method further including:

in the event of tampering with the PSD, removing power from the third memory resulting in a loss of the decrypted body of data.

Grider et al. teaches for, a security improvement against tempering, that the improvement includes: a micro-controller supplies power to the memory either from a system power supply or from the battery, and grounds the power-output to the memory to destroy all data in the memory (col. 2, lines 1-6).

Since Grider et al. and Rager et al. are both from the same field of endeavor of providing security measure against tempering for the memory, the purpose disclosed by Grider et al. would have been well recognized in the pertinent field of Rager et al..

Accordingly, it would have been obvious at the time the invention was made to a person having ordinary skill in the art, to not only remove power from the second memory, which is supplied with the power even after the device is powered down, but also remove the power from the third memory, which is only supplied with the power during the power ups of the device, as taught by Grider et al., for the purpose of providing a device with improved security against tempering, including attempts at active intrusion while the machine is running (Rager et al. already prevents the device from tempering when powered downs and with teaching of Grider et al. the modified Rager et al. can further prevent the tempering against active intrusion during the power ups).

W.R.T. Claim 9:

Rager et al. discloses a device comprising:

Art Unit: 3629

a second volatile memory (106) for storing the encryption key (in Fig. 1; col. 4, lines 17-20), wherein a constant voltage is supplied to the encryption device and consequently to the second memory (col. 4, lines 37-40) when the device is powered down;

a first nonvolatile memory (130) not having a backup power batter for storing the encrypted body of data in the first memory (103 in Fig. 1, col. 4, lines 8-10);

an encryption engine (105) for encrypting the body of data with respect to the encryption key (col. 3, lines 27-34);

a third memory not having a backup battery for temporarily storing the decrypted body of data (102 in Fig. 1; col. 4, lines 31-32, 35-36); and

wherein upon power down of the device the decrypted body of data in the third memory is lost.

However, Rager et al. does not expressly disclose:

what kind of backup power is supplied to the second memory device (is it a backup battery power source or other power source?); and

in the event of tampering with the PSD, removing power from the third memory resulting in a loss of the decrypted body of data.

Grider et al. teaches for, a security improvement against tempering, that the improvement includes: the memory is getting power source either from a system power

Art Unit: 3629

supply or from the backup battery (col. 2, lines 1-6); and a micro-controller grounds the power-output to the memory to destroy all data in the memory (col. 2, lines 1-6).

Since Grider et al. and Rager et al. are both from the same field of endeavor of providing security measure against tempering for the memory, the purpose disclosed by Grider et al. would have been well recognized in the pertinent field of Rager et al..

Accordingly, it would have been obvious at the time the invention was made to a person having ordinary skill in the art, to supply power to second memory from the backup battery in case the device is powered down; and to not only remove power from the second memory, which is supplied with the power even after the device is powered down, but also remove the power from the third memory, which is only supplied with the power during the power ups of the device, as taught by Grider et al., for the purpose of maintaining security while the security device is powered down and providing a device with improved security against tempering, including attempts at active intrusion while the machine is running (Rager et al. already prevents the device from tempering when powered downs and with teaching of Grider et al. the modified Rager et al. can further prevent the tempering against active intrusion during the power ups).

The modified device of Rager et al. discloses the invention as recited above, but does not specifically disclose that the second memory is a nonvolatile type.

At the time the invention was made, it would have been an obvious matter of design choice to a person of ordinary skill in the art to substitute the nonvolatile memory in place of the volatile memory because Applicant has not disclosed that utilizing the nonvolatile memory instead of volatile one provides an advantage, is used for a particular purpose, or solves a stated problem. One of ordinary skill in the art, furthermore, would have expected Applicant's invention to perform equally well with the second volatile memory of Rager et al. because the data in the second volatile memory of Rager et al. will also be erased if the device is tempered.

Therefore, it would have been an obvious matter of design choice to further modify the modified device of Rager et al. to obtain the invention as specified in claim.

W.R.T. Claim 10: The modified device of Rager et al. further discloses the device adapted to interrupt power to the second memory device and the third memory device, wherein the body of decrypted data is lost and the encryption key is not available.

W.R.T. Claim 12:

Rager et al. discloses a method comprising the steps of:

storing the encryption key within the second memory (106, in Fig. 1; col. 4, lines 17-20);

encrypting the body of data by the cryptographic engine (105) with respect to the encryption key (col. 3, lines 27-34);

Art Unit: 3629

storing the encrypted body of data in the first memory (103 in Fig. 1, col. 4, lines 8-10);

upon power-up of the security device decrypting the encrypted body of data with the cryptographic engine with respect to the encryption key (col. 4, lines 23-27);

temporarily storing the decrypted body of data in a third memory (102 in Fig. 1; col. 4, lines 31-32, 35-36), wherein upon power down of the device the decrypted body of data is lost; and

in the event of tampering with the device, removing power from the second memory resulting in a loss of the encryption key and the decrypted body of data (see col. 4, lines 44-49).

However, Rager et al. does not expressly disclose:

what kind of backup power is supplied to the second memory device (is it a backup battery power source or other power source?); and

in the event of tampering with the PSD, removing power from the third memory resulting in a loss of the decrypted body of data.

Grider et al. teaches for, a security improvement against tempering, that the improvement includes: the memory is getting power source either from a system power supply or from the backup battery (col. 2, lines 1-6); and a micro-controller grounds the power-output to the memory to destroy all data in the memory (col. 2, lines 1-6).

Since Grider et al. and Rager et al. are both from the same field of endeavor of providing security measure against tempering for the memory, the purpose disclosed by Grider et al. would have been well recognized in the pertinent field of Rager et al..

Accordingly, it would have been obvious at the time the invention was made to a person having ordinary skill in the art, to supply power to second memory from the backup battery in case the device is powered down; and to not only remove power from the second memory, which is supplied with the power even after the device is powered down, but also remove the power from the third memory, which is only supplied with the power during the power ups of the device, as taught by Grider et al., for the purpose of maintaining security while the security device is powered down and providing a device with improved security against tempering, including attempts at active intrusion while the machine is running (Rager et al. already prevents the device from tempering when powered downs and with teaching of Grider et al. the modified Rager et al. can further prevent the tempering against active intrusion during the power ups).

W.R.T. Claim 13: The modified method of Rager et al. further includes: generating an electrical signal when the device is tampered with that causes the second memory and the third memory to clear their respective memories (see Supra columns regarding the tempering).

W.R.T. Claim 14: The modified method of Rager et al. further include: interrupting main electrical power and back-up battery power to the memories if the device is tampered with (see Supra Grider et al. for interrupting both sources of power).

Art Unit: 3629

W.R.T. Claim 15: The modified method of Rager et al. would minimize an amount of backup battery power consumed by the device because the only second memory is powered by the battery.

W.R.T. Claim 16: The modified method Rager et al. would disclose that only the encryption key and the encrypted body of data are stored when the device is powered down because the first (nonvolatile) and second memory (backup battery) are not effected by simple power down.

6) Claims 5, 7-8, 11, 17-18 and 21 rejected under 35 U.S.C. 103(a) as being unpatentable over Rager et al. and Grider et al. as applied to claims 4, 6, 9, 12 above, and further in view of Kubatzki et al. (US 5,771,348).

The modified Rager et al. discloses the invention as recited earlier, but does not expressly disclose that the device is used for a postage meter such that the meter prints data for the printing of postal indicia, and sends a message via a communication channel to a postal authority.

Kubatzki et al is cited to show how the security device can be implemented into the postage meter, wherein the critical data is protected against manipulation.

Accordingly, it would have been obvious at the time the invention was made to a person having ordinary skill in the art to replace the existing security device of Kubatzki et al. with the security device of Rager et al. such that the meter prints data for the printing of postal indicia, which is well protected under the security device of Rager et al.

Art Unit: 3629

and contacts the postal authority when tempered by utilizing the communication channel available at the postage meter of Kubatzki et al., for the purpose of enhancing the security of critical data (e.g. postal indicia image data) against manipulation.

Allowable Subject Matter

7) Claims 19-20 are objected to as being dependent upon a rejected base claim, but would be allowable if rewritten in independent form including all of the limitations of the base claim and any intervening claims.

Conclusion

8) Any inquiry concerning this communication or earlier communications from the examiner should be directed to Richard Woo whose telephone number is 703-308-7830. The examiner can normally be reached on Monday-Friday from 8:30 AM -5:00 PM.

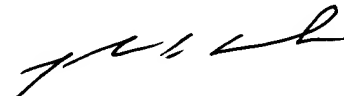
If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, John Weiss can be reached on 703-308-2702. The fax phone number for the organization where this application or proceeding is assigned is 703-872-9306.

Art Unit: 3629

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see <http://pair-direct.uspto.gov>. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).



Richard Woo
Patent Examiner
Art Unit 3629
February 5, 2005



JOHN G. WEISS
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 3600